# Configurar Alta Disponibilidade de FTD Usando FDM

Contents
Introdução
<u>Pré-requisitos</u>
Requisitos
Componentes Utilizados
Topologia de rede
Configurar
Configurar a Unidade Principal para Alta Disponibilidade
Configurar a unidade secundária para alta disponibilidade
Verificar

## Introdução

Este documento descreve como configurar um par de HA (High Availability, alta disponibilidade) ativo/standby de FTD (Secure Firewall Threat Defense, defesa contra ameaças de firewall) gerenciado localmente.

## Pré-requisitos

#### Requisitos

Recomenda-se ter conhecimento destes tópicos:

• Configuração inicial do Cisco Secure Firewall Threat Defense via GUI e/ou shell.

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

• FPR2110 versão 7.2.5 gerenciado localmente pelo Firepower Device Manager (FDM)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

### Topologia de rede



Observação: o exemplo descrito neste documento é um dos vários projetos de rede recomendados. Consulte o guia de configuração <u>Como evitar failover interrompido e links</u> <u>de dados</u> para obter mais opções.



## Configurar

Configurar a Unidade Principal para Alta Disponibilidade

Etapa 1. Clique em Device e pressione o botão Configure no canto superior direito, ao lado do status High Availability (Alta disponibilidade).



Etapa 2. Na página High Availability (Alta disponibilidade), clique na caixa Primary Device.



Etapa 3. Configure as propriedades do Link de Failover.

Selecione a interface conectada diretamente ao firewall secundário e defina o endereço IP primário e secundário, bem como a sub-rede Netmask.

Marque a caixa de seleção Usar a mesma interface que o link de failover para o link de failover stateful.

Desmarque a caixa Chave de criptografia IPSec e clique em Ativar HA para salvar as alterações.

I have configuration of peer device in clipboard PASTE FROM CLIPBOARD	
FAILOVER LINK	STATEFUL FAILOVER LINK Use the same interface as the Failover Link
Interface	Interface
unnamed (Ethernet1/7) V	unnamed (Ethernet1/7) ~
Type IPv4 IPv6 Primary IP 10.1.1.1	Type IPv4 IPv6 Primary IP 10.1.1.1
e.g. 192.168.10.1	e.g. 192.168.11.1
Secondary IP 10.1.1.2 e.g. 192.168.10.2	Secondary IP 10.1.1.2 e.g. 192.168.11.2
Netmask	Netmask
255.255.255.252	255.255.255.252
e.g. 255.255.255.0 or 24	e.g. 255.255.255.0 or 24
IPSec Encryption Key (optional) For security purposes, the encryption key will not be included in the configuration copied to the clipboard when you activate HA. You will need to manually enter the key when you configure HA on the peer device.	IMPORTANT If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More
Before you activate HA, make sure both devices have the same Smart License and Cloud Regi	on. Otherwise HA will not work.
When you click Activate HA, these settings are automatically deployed to the dev momentary traffic loss. It might take a few minutes for deployment to finish.	ice. The deployment might restart inspection engines, which can result in the
Information is copied to the clipboard when deployment is done. You must allow the clipboard when deployment is done.	the browser to access your clipboard for the copy to be successful.





Dica: use uma sub-rede de máscara pequena, dedicada ao tráfego de failover somente para evitar violações de segurança e/ou problemas de rede o máximo possível.



Aviso: o sistema implanta imediatamente a configuração no dispositivo. Não é necessário iniciar um trabalho de implantação. Se você não vir uma mensagem informando que sua configuração foi salva e a implantação está em andamento, role para a parte superior da página para ver as mensagens de erro. A configuração também é copiada para a área de transferência. Você pode usar a cópia para configurar rapidamente a unidade secundária. Para maior segurança, a chave de criptografia (se você definir uma) não é incluída na cópia da área de transferência.

Etapa 4. Após a conclusão da configuração, você receberá uma mensagem explicando as próximas etapas. Depois de ler as informações, clique em Got It.

the	You have successfully deployed HA configuration on the primary device. What's next? need to configure Peer Device I configured both devices	×
	Copy the HA configuration to the clipboard. Copied Click here to copy again Paste it on the secondary device.	
	Log into the secondary device and open the HA configuration page.         You are done!         The devices should communicate and establish a high availability pair automatically.	
	GOT IT	

Configurar a unidade secundária para alta disponibilidade

Etapa 1. Clique em Device e pressione o botão Configure no canto superior direito, ao lado do status High Availability (Alta disponibilidade).

Firewall Device Manager Monitoring	Policies Object:	s Device: ftd-secondary		adr	nin 🗸 🖞 讨 SECURE
Model Cisco Firepower 2110 Thr	Software eat Defense 7.2.5-208	VDB Intrusion Rule Update 0 370.0 20230925-1455	Cloud Services	High Availability @ C	ONFIGURE
FC Inside Network	Cisco Firepower 2110 Thr MGMT 1/1 CONSOLE 1/2	12 est Defense 1/3 1/5 1/7 1/9 1/11 1/13 1/ 1/13 1/ 1/14 1/5 1/8 1/11 1/15 1/7 1/9 1/11	/14 1/15 1/16	SP/WAN/Gateway	Internet DNS Server NTP Server Smart License

Etapa 2. Na página Alta disponibilidade, clique na caixa Dispositivo secundário.

Firewall De	vice Manager Monitoring	Ø Policies	註王 Objects	Device: ftd-secondary	E		0	?	admin Administrato	v dha cisc	SECURE
	Device Summary High Availability										
	How High Availability Work	s								~	
Select the role for this device The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first. The secondary device remains in standby mode until the primary unit becomes unavailable.											
			P	rimary Device or	Secondary Devic	•					

Etapa 3. Configure as propriedades do Link de Failover. Você pode colar as configurações armazenadas na área de transferência após configurar o FTD primário ou pode continuar manualmente.

Etapa 3.1. Para colar da área de transferência, basta clicar no botão Colar da área de transferência, colar na configuração (pressione as teclas Ctrl+v simultaneamente) e clicar em OK.

Select the role for this device					
The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first. The secondary device remains in standby mode until the primary unit becomes unavailable.					
Primary Device     or     Secondary Device     @					
I have configuration of peer device in clipboard PASTE FROM CLIPBOARD					

```
Paste here Peer Device Configuration

FAILOVER LINK CONFIGURATION

Therface: Ethernet1/7

Primary IP: 10.1.1.1/255.255.252

Secondary IP: 10.1.1.2/255.255.252

STATEFUL FAILOVER LINK CONFIGURATION

Therface: Ethernet1/7

Primary IP: 10.1.1.1/255.255.255.252

Secondary IP: 10.1.1.2/255.255.255.252
```

Etapa 3.2. Para continuar manualmente, selecione a interface conectada diretamente ao firewall secundário e defina o endereço IP primário e secundário, bem como a sub-rede Netmask. Marque a caixa de seleção Usar a mesma interface que o link de failover para o link de failover stateful.

I have configuration of peer device in clipboard	PASTE FROM CLIPBOARD		
FAILOVER LINK		STATEFUL FAILOVER LINK	Use the same interface as the Fallover Link
Interface		Interface	
unnamed (Ethernet1/7)	~	unnamed (Ethernet1/7)	~
Type IPv4 IPv6		Type IPv4 IPv6	
Primary IP		Primary IP	
10.1.1.1		10.1.1.1	
Secondary IP 10.1.1.2		Secondary IP 10.1.1.2	
e.g. 192.168.10.2		e.g. 192.168.11.2	
Netmask		Netmask	
255.255.255.252		255.255.255.252	
e.g. 255.255.255.0 or 24		e.g. 255.255.255.0 or 24	
IPSec Encryption Key (optional) For security purposes, the encryption key will not be includ clipboard when you activate HA. You will need to manually enter the key when you configure	ed in the configuration copied to the HA on the peer device.	IMPORTANT If you configure an IPsec encryption k features, both devices will become ac	ey with inconsistent settings for export controlled tive after you activate HA. Learn More 🕑
Before you activate HA, make sure both devices hav	e the same Smart License and Cloud Regi	ion. Otherwise HA will not work.	
when you click Activate HA, these settings a momentary traffic loss. It might take a few m	re automatically deployed to the dev nutes for deployment to finish.	vice. The deployment might restart insp	pection engines, which can result in the
Information is copied to the clipboard when a	deployment is done. You must allow	the browser to access your clipboard	for the copy to be successful.
	ACTIV	ATE HA	

Etapa 4. Desmarque a caixa Chave de criptografia IPSec e clique em Ativar HA para salvar as alterações.



Aviso: o sistema implanta imediatamente a configuração no dispositivo. Não é necessário iniciar um trabalho de implantação. Se você não vir uma mensagem informando que sua configuração foi salva e a implantação está em andamento, role para a parte superior da página para ver as mensagens de erro.

Etapa 5. Após a conclusão da configuração, você receberá uma mensagem explicando as próximas etapas que devem ser executadas. Depois de ler as informações, clique em Got It.

You have successfully deployed the HA configuration on the primary device. What's next?	×
<ul> <li>Copy the HA configuration to the clipboard.</li> <li>Copied Click here to copy again</li> <li>Paste it on the secondary device.</li> <li>Log into the secondary device and open the HA configuration page.</li> </ul>	
You are done! The devices should communicate and establish a high availability pair automatically.	
GOT IT	

## Verificar

 Nesse ponto, a maioria dos status do dispositivo indica que esse é o dispositivo secundário na página Alta disponibilidade. Se a junção com o dispositivo primário foi bem-sucedida, o dispositivo começa a sincronizar com o primário e, eventualmente, o modo é alterado para Standby e o peer para Ative.

This device is part of a high availability (HA) pair and is currently in standby state. With few exceptions, you cannot edit the configuration for this device. To make any changes, please log into the active unit. Learn More C							
Firewall Device Manager	Monitoring Policies Objects	Device: ftd-primary	admin v studio SECURE				
	Model Cisco Firepower 2110 Threat	Software VDB Intrusion Rule Update Cloud Services Defense 7.2.5-208 370.0 20230925-1455 Ocnnected   SEC TAC	High Availability Secondary Device: Standby 🛛 🤃 Peer: Active				
	Finiside Network	Internet DNS Server ISP/WAN/Gateway C NTP Server Smart License					

• O FTD Principal também deve mostrar o status de Alta Disponibilidade, mas como Ativo e Par: Em Espera.

Firewall Device Manager Monite	ring Policies Objects Devi	ce: ftd-primary	) de 🗐 ? :	admin Administrator
	Model Cisco Firepower 2110 Threat Defense	Software VD8 Intrusion Rule Update Clou 7.2.5-208 370.0 20230925-1455 🥑 C	d Services High Availability Primary Device: Active	₽ Peer: Standby
	Cisco Fi	1/2 Nepower 2110 Threat Defense 🛈		Internet
	C Inside Network	MAMT 1/1 1/2 1/5 1/7 1/9 1/11 CONSOLE 1/2 1/4 1/6 1/8 1/10 1/12 SFP	4 1/15 1/16 ISP/WAN/Gateway	NTP Server
		<b>17</b>		

 Abra uma sessão SSH para o FTD principal e emita o comando show running-config failover para verificar a configuração.



• Valide o status atual do dispositivo com o comando show failover state.

> show failover state					
This host -	State Primary	Last	Failure	Reason	Date/Time
Other host -	Active Secondary	None			
	Standby Ready	None			
====Configurat:	ion State===				
Mac se	t				
>					

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.